I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Foreword: The NSA and the Legal Regime for Foreign Intelligence Surveillance

PETER M. SHANE[1]

"Mr. President, no one is saying you broke any laws, we're just saying it's a little bit weird you didn't have to."

- John Oliver[2]

As the papers in this symposium[3] and conflicting lower court opinions[4] demonstrate, serious commentators reviewing the National Security Agency (NSA) surveillance programs that have been revealed through recent leaks are far from unanimous that the programs are

---

[1]Jacob E. Davis and Jacob E. Davis II Chair in Law, Moritz College of Law, Ohio State University. I am grateful to the symposium authors and to my colleague Dakota Rudesill for valuable feedback on earlier versions of this manuscript.

[2] *The Daily Show: Good News! You're Not Paranoid –NSA Oversight* (Comedy Central Broadcast, June 10, 2013), *available at* http://www.thedailyshow.com/watch/mon-june-10-2013/the-daily-show-with-john-oliver.

[3] *Compare* John Yoo, *The Legality of the National Security Agency's Bulk Data Surveillance Programs*, 10 ISJLP 301-326 (2014) (defending NSA surveillance), *with* Katherine Strandburg, *Membership Lists, Metadata, and Freedom of Association's Specificity Requirement*, 10 ISJLP 327-365 (2014) (challenging NSA metadata collection under the First Amendment) and Laura Donohue, *PRISM and the Interception of Communications Under Section 702 of the Foreign Intelligence Surveillance Act*, 10 ISJLP 599-639 (2014) (challenging NSA's current programs of electronic surveillance under the Fourth Amendment). On possible statutory challenges to the legality of the metadata collection programs, see text at notes 7-18, *infra*.

[4] *Compare* ACLU v. Clapper, No. 13 Civ. 3994 (S.D.N.Y., Dec. 27, 2013) (upholding against Fourth Amendment challenge the NSA's bulk collection of telephone metadata), *with* Klayman v. Obama, No. 13 Civ 0851(RJL) (D.D.C., Dec. 16, 2003) (finding the NSA's bulk collection of telephone metadata in violation of the Fourth Amendment).

lawful. The point of John Oliver's joke, however, still rings true: Somehow, our laws have evolved to a stage where lawyers could plausibly defend the government's entitlement to capture and store an immense volume of our telephone and online communications, as well as metadata about both. For many Americans, this is a breathtaking reality. The point of this article is to explain our legal evolution as a way of providing context for the *I/S* symposium on "NSA Surveillance: Security, Privacy, and Civil Liberty." It will introduce the papers that follow, and offer some concluding thoughts on the issues of executive power that lurk behind the controversy. Specifically, I want to suggest that what may seem like an oddly mixed performance record in the history of the Foreign Intelligence Surveillance Court may best be explained as a reflection of that court's willingness to indulge in surprisingly expansive executive branch readings of the government's statutory surveillance authority in order to maintain some significant judicial leverage to protect privacy in the administrative implementation of that authority. As unsatisfactory an institutional compromise as this may seem in principle, it may be better than having an executive branch that thinks itself beholden only to its own construction of its inherent constitutional powers.

I. INTERCEPTING COMMUNICATION CONTENTS: FROM *OLMSTEAD* TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

Prior to the late 1960s, the federal government did not interpret law as constraining its entitlement to collect the contents of communications through electronic surveillance for either criminal investigation or national security purposes. The Supreme Court had held in 1928 that a wiretap was not a Fourth Amendment "search," because it involved neither physical trespass, nor the seizure of a tangible thing.[5] Three years later, Attorney General William D. Mitchell issued the first authorization for telephone wiretapping, then aimed at syndicated bootleggers.[6]

In 1934, Congress enacted a legal ban on wiretaps, providing in the Federal Communications Act that it would be a felony for any person "to intercept and divulge or publish the contents of wire and radio communications."[7] Although the Supreme Court held the

---

[5] Olmstead v. United States, 277 U.S. 438, 468 (1928).

[6] Foreign Intelligence Surveillance Act of 1978, H.R. REP. NO. 95-1283, pt. 1 (1978) (hereinafter, "House FISA Report").

[7] 47 U.S.C. § 605 (effective Feb. 8, 1996).

prohibition applicable to federal agents[7]–thus rendering wiretap evidence inadmissible at trial–the Justice Department interpreted the law and the Court's decisions as forbidding only the public divulgence of intercepted communications, not wiretapping itself.[8] As a result, when President Roosevelt informed the Attorney General in 1940 of his view that counterintelligence wiretaps were constitutional, the Justice Department did not perceive any Fourth Amendment bar to their use for national security purposes.[9]

The government expanded its use of national security wiretaps from the Roosevelt through the Nixon Administrations. The Truman Administration even abandoned the Roosevelt policy of limiting its targets "insofar as possible" to aliens.[10] The Eisenhower Administration took the position that surreptitious physical entry to conduct wiretapping was likewise legally authorized.[11] As recounted in a House report: "From the relatively limited authorization of warrantless electronic surveillance under President Roosevelt . . . the mandate for the FBI was quickly expanded to the point where the only criterion was the FBI's subjective judgment that the 'national interest' required the electronic surveillance."[12]

With two critical decisions, however, the Supreme Court radically changed the relevant legal landscape. The Court's 1967 decision in *Katz v. United States*[13] overruled *Olmstead* and applied the Fourth Amendment's warrant provision to electronic surveillance in connection with a criminal prosecution. Congress responded by enacting Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[14] creating standards to govern, and a process for obtaining, criminal wiretap warrants. The Act explicitly provided, however, that it worked no change in the President's authority to engage in surveillance "to obtain foreign intelligence information deemed

---

[7] Nardone v. United States, 302 U.S. 379 (1937); Nardone v. United States, 308 U.S. 338 (1939).

[8] House FISA Report, *supra* note 6, at 15.

[9] *Id.*

[10] *Id.* at 16.

[11] *Id.*

[12] *Id.*

[13] 389 U.S. 347 (1967).

[14] Pub. L. No. 90-351, § 801, 82 Stat. 197, 211-218 (1968) (codified as amended at 18 U.S.C. §§ 2510-2520 (2012)).

essential to the security of the United States, or to protect national security information against foreign intelligence activities."[15]

Notwithstanding this disclaimer, the Supreme Court proceeded to decide, in the 1976 *Keith* case,[16] that warrantless surveillance was also unconstitutional in the context of wholly domestic national security investigations. At least where "[t]here is no evidence of any involvement, directly or indirectly, of a foreign power,"[17] the Court found no categorical exception to the warrant requirement. In balancing the competing values at stake, the Court observed: "Though the investigative duty of the executive may be stronger in [national security] cases, so also is there greater jeopardy to constitutionally protected speech."[18]

The *Keith* Court went beyond its Fourth Amendment holding to opine that the requirement of prior magistrate approval for national security warrants did not demand that such warrants be issued only on grounds identical to Title III criminal prosecution warrants.[19] The Court expressly invited Congress to tackle the problem, stating: "Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens."[20]

Congress's acceptance of the Court's invitation, however, was colored by revelations in 1975 and 1976 that the CIA, FBI, and other intelligence-gathering units within the executive branch had engaged in massive, illegal domestic intelligence operations during the Nixon administration.[21] Reports of CIA abuse led President Ford to name an eight-member commission (including future President Reagan) under

---

[15] Pub. L. No. 90-351, § 802, 82 Stat. 197, 212 (1968) (codified at 18 U.S.C. § 2511(3)).

[16] United States v. United States District Court, 407 U.S. 297 (1972). The case is commonly known by the name of the U.S. District Court Judge whose order was under review.

[17] *Id.* at 309.

[18] *Id.* at 313.

[19] *Id.* at 322.

[20] *Id.*

[21] Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities – Book 2: Intelligence Activities and the Rights of Americans, S. REP. NO. 94-755, at 1-20 and passim (1976); *see generally* Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities – Book 3: Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans, S. REP. NO. 94-755 (1976).

Vice President Rockefeller to investigate alleged CIA statutory violations.[22] On January 15, 1975, CIA Director William Colby presented a lengthy report to the Senate Appropriations Intelligence Operations Subcommittee, acknowledging that the CIA had carried out surveillance of journalists and political activists, opened the mail of U.S. citizens, infiltrated domestic protest groups and gathered information for secret files on more than 10,000 Americans.[23] Twelve days later, the Senate established an eleven-member select committee under Senator Frank Church ("Church Committee") to investigate the activities of the CIA, FBI, and other law enforcement and intelligence agencies to determine if they had engaged in any illegal or unethical intelligence activities during the Vietnam period.[24] (A parallel study was later undertaken in the House of Representatives, under Rep. Otis G. Pike, of New York.)[25]

What followed in the wake of *Keith* and the Church Committee report was an intense interbranch collaboration between Congress and, first, the Ford Administration, later the Carter Administration, on the drafting of what became the Foreign Intelligence Surveillance Act of 1978 (FISA).[26] FISA was enacted on Congress's understanding, in which Attorneys General Levi and Bell concurred, that "Congress has at least concurrent authority to enable it to legislate with regard to the foreign intelligence activities of departments and agencies of this Government either created or funded by Congress."[27] As described in

---

[22] REPORT TO THE PRESIDENT BY THE COMMISSION ON CIA ACTIVITIES WITHIN THE UNITED STATES, at ix (1975).

[23] Senate Committee on Intelligence Activities: Report of the Committee on Government Operations to Accompany S. Res. 400 Resolution to Establish a Standing Committee of the Senate on Intelligence Activities, And For Other Purposes, S. REP. NO. 94-675 at 4 (1976).

[24] Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities – Book 1: Foreign and Military Intelligence, S. REP. NO. 94-755 at 2-3 (1976).

[25] Gerald K. Haines, *The Pike Committee Investigations and the CIA: Looking for a Rogue Elephant*, STUD. INTELLIGENCE 81-92 (Winter 1998-99), *available at* https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol42no5/pdf/v42i5a07p.pdf.

[26] Pub. L. No. 95-511, 92 Stat. 1783 (1978); House FISA Report, *supra* note 6, at 13-14. For a history of the drafting of FISA by a law professor who, as a government lawyer, was directly involved in its development, see William Funk, *Electronic Surveillance of Terrorism: The Intelligence/Law Enforcement Dilemma – A History*, 11 LEWIS & CLARK L. REV. 1099 (2007). For a thoughtful journalistic account of the history of executive branch and congressional interaction over the legal control and oversight of national security surveillance, see Ryan Lizza, *State of Deception*, NEW YORKER, Dec. 16, 2013, at 48.

[27] House FISA Report, *supra* note 6, at 24.

a House committee report, Congress's "presumption" in designing FISA was that "whenever an electronic surveillance for foreign intelligence purposes may involve the fourth amendment rights of any U.S. person, approval for such a surveillance should come from a neutral and impartial magistrate."[28]

Even in its original form, FISA was a dauntingly complex statute. It created an entirely new and unprecedented institution–the Foreign Intelligence Surveillance Court (FISC)–to superintend the process of authorizing foreign intelligence surveillance.[29] The FISC's membership, designated by the Chief Justice of the United States, comprises 11 district court judges who must represent at least seven of the United States judicial circuits. In addition, the Chief Justice designates three judges–from either the district courts or courts of appeals–to constitute a review panel to which the United States may appeal any FISC decision denying a warrant application. The court's novelty, other than in its membership and selection, lay in its secrecy. Its proceedings are entirely ex parte; should the Government petition for certiorari review of any decision adverse to the Government that is upheld on appeal, what is now called the FISC Court of Review transmits the record of the matter to the Supreme Court under seal.[30]

Hidden in FISA's definitional sections, as well as in its operative provisions, were a host of important policy decisions regarding the scope of permissible surveillance. One was to permit the Attorney General to authorize warrantless foreign intelligence surveillance, for a year at a time, where directed exclusively at communications between foreign powers;[31] conversely, no authority was provided at all under FISA for national security investigations that lacked any international or foreign dimension. As a result, electronic surveillance directed at a wholly domestic national security threat, as in *Keith*, must still be authorized under the Title III probable cause standard.

For electronic surveillance directed at foreign intelligence, however–assuming it is not exclusively between "foreign powers" as defined in the Act–FISA makes a critical concession to the executive branch in relaxing the standard for a surveillance warrant. Specifically, it is not necessary, as with a Title III warrant, that probable cause exist to believe the surveillance will yield evidence of a crime; in applying for a FISA warrant, the Attorney General has to

---

[28] *Id.* at 24-25.

[29] Pub. L. No. 95-511, § 103, 92 Stat. 1788 (1978), codified at 50 U.S.C. § 1803.

[30] *Id.* at § 1803(a).

[31] Pub. L. No. 95-511, § 102, 92 Stat. 1786 (1978), codified at 50 U.S.C. § 1802(a)(1).

certify instead that "the purpose of the surveillance is to obtain foreign intelligence information" and the official certifying the warrant application to the Foreign Intelligence Surveillance Court "deems the information sought to be foreign intelligence information."[32]

The character of the information sought, however, is not sufficient by itself to sustain a FISA warrant application. A FISA warrant–and thus the relaxation of the probable cause standard–is available to the government only if "the target of the electronic surveillance is a foreign power or an agent of a foreign power."[33] "United States persons"–essentially, citizens and lawfully resident aliens–cannot literally be "foreign powers," although surveillance directed at a foreign power may cover such persons if they belong to a faction of a foreign nation or nations, a group engaged in or preparing for international terrorism, or a foreign-based political organization.[34] Americans may also be targeted for surveillance if they are "agents of

---

[32] Pub. L. No. 95-511, § 104, 92 Stat. 1788 (1978), codified at 50 U.S.C. §§ 1804(a)(6)(A) and (B). The USA PATRIOT Act, Pub. L. No.107-56, § 218, 115 Stat. 291 (2001) changed "the purpose" in 50 U.S.C. § 1804(a)(6)(B) to "a significant purpose."

FISA originally defined "foreign intelligence information," as follows:

> (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against–,
>
> (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
>
> (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
>
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
>
> (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to–
>
> (A) the national defense or the security of the United States; or
>
> (B) the conduct of the foreign affairs of the United States.

Pub. L. No. 95-11, § 101, 92 Stat. 1783 (1978), codified as amended at 50 U.S.C. § 1801(e) (1982). In 2008, "sabotage or international terrorism" in subparagraph (1)(B) was deleted and "sabotage, international terrorism, or the international proliferation of weapons of mass destruction" inserted in its place. Pub. L. 110-261, § 110(a), 122 Stat. 2466 (2008).

[33] Pub. L. No.95-511, § 104(a)(4)(A), 92 Stat. 1789 (1978), codified as amended at 50 USC § 1804(a)(4)(A).

[34] Pub. L. No. 95-511, § 101(a), 92 Stat. 1783, codified as amended at 50 U.S.C. § 1801(a).

a foreign power." This would include persons who knowingly aid and abet acts in preparation for international terrorism.[35]

But perhaps FISA's most obscure policy choices are embedded in its definition of "electronic surveillance."[36] The definition of "electronic surveillance" was written to cover several categories of information acquisition by "an electronic, mechanical, or other surveillance device." Such a device is covered categorically if used to intercept "any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States."[37] If used to intercept the contents of any radio communication, such a device is covered if the interception was

---

[35] "Agent of a foreign power" means–

> (1) any person other than a United States person, who–
>
> (A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a) (4);
>
> (B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or
>
> (2) any person who–
>
> (A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statues of the United States;
>
> (B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;
>
> (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power; or
>
> (D) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

Pub. L. No. 95-511, § 101(b), 92 Stat. 1783, codified as amended at 50 U.S.C. § 1801(b).

[36] Pub. L. No. 95-511, § 101(f), 92 Stat. 1785, codified as amended at 50 U.S.C. § 1801(f).

[37] *Id.* at § 101(f)(2), 92 Stat. 1785, codified as amended at 50 U.S.C. § 1801(f)(2).

intentional and "under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States."[38] With regard to both wire and radio communications, interception is covered with regard to any "communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes."[39]

What these definitions may well obscure for the uninitiated reader are the categories of what is, in fact, electronic surveillance, but that FISA apparently permits to proceed without warrants. Most notably, communications wholly outside the United States are exempt, no matter who participates. Also, acquisitions of radio (i.e., wireless) communications are not covered unless they occur "under circumstances in which a person has a reasonable expectation of privacy," circumstances that legislators expected would not cover, for example, citizens band or ham radio transmissions.[40]

What also may not be obvious is that Congress understood the coverage for "the *contents* of any wire communication to or from a person in the United States" to include what is now commonly called metadata, i.e., information identifying the calling and receiving devices involved in a communication and indicating the length of that communication. In identical language, the relevant committee reports stated:

> The surveillance covered by subparagraph (B) is not limited to the acquisition of the oral, or verbal contents of a wire communication. It includes the acquisition of any other contents of the communication, for example, where computerized data is transmitted by wire. Therefore, it includes any form of "pen register" or

---

[38] *Id.* at § 101(f)(3), 92 Stat. 1785, codified as amended at 50 U.S.C. § 1801(f)(3).

[39] *Id.* at § 101(f)(1), 92 Stat. 1785, codified as amended at 50 U.S.C. § 1801(f)(1). The fourth definition encompasses "the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes." *Id.* at § 101(f)(4), 92 Stat. 1785, codified as amended at 50 U.S.C. § 1801(f)(4).

[40] House FISA Report, *supra* note 6, at 52.

> "touch-tone decoder" device which is used to acquire, from the contents of a wire communication, the identities or locations of the parties to the communication.[41]

Because the legislative history as well as the statutory language of FISA was the subject of intense interbranch negotiation, it is reasonable to expect that the Justice Department subsequently interpreted FISA to permit pen register warrants as well.

II. BULK INFORMATION, ECPA AND THE USA PATRIOT ACT

The devices that capture information about communications one initiates are called "pen registers."[42] Devices that capture such information about communications people receive are called "trap and trace" devices.[43] Despite FISA's tacit reference to "electronic devices" used to capture information about communications apart from their actual contents, it was not until eight years later that Congress regulated the use of such devices comprehensively. Congress regulated both pen registers and trap and trace devices under the Electronic Communications Privacy Act of 1986 (ECPA), which prohibited the use of such devices except pursuant to either a FISA

---

[41] House FISA Report, *supra* note 6, at 51; Foreign Intelligence Surveillance Act of 1978, S. REP. NO. 95-701 at 35 (1978).

[42] Under the Electronic Privacy Communication Act, "the term 'pen register' means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business." Pub. L. No. 99–508, § 301(a), 100 Stat. 1870 (1986), codified as amended at 18 U.S.C. § 3127(3). (Provisions of the ECPA that, as of 1986, were codified at 18 U.S.C. §§ 3125-3126 were renumbered §§ 3126-3127 with the addition of a new § 3125 in 1988. Pub. L. No.100-690, § 7092(a)(2), 102 Stat. 4410 (1988).)

[43] Under the Electronic Communications Privacy Act, "the term 'trap and trace device' means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication." *Id.*, codified as amended at 18 U.S.C. § 3127(4).

warrant or ECPA itself.[44] Notably, however, the standard for obtaining a pen register warrant under ECPA is arguably even less demanding than the FISA standard. The applicant agency for such a warrant need certify only "that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency."[45]

In 1998, Congress made explicit that FISA authorized pen register and trap and trace warrants and expanded the scope of that authority. Under Section 601 of the Intelligence Authorization Act for Fiscal Year 1999, the government may get such a device based on:

> information which demonstrates that there is reason to believe that the telephone line to which the pen register or trap and trace device is to be attached, or the communication instrument or device to be covered by the pen register or trap and trace device, has been or is about to be used in communication with—
>
> (A) an individual who is engaging or has engaged in international terrorism or clandestine intelligence activities that involve or may involve a violation of the criminal laws of the United States; or
>
> (B) a foreign power or agent of a foreign power under circumstances giving reason to believe that the communication concerns or concerned international terrorism or clandestine intelligence activities that involve or may involve a violation of the criminal laws of the United States.[46]

---

[44] Pub. L. No. 99-508, § 301(a), 100 Stat. 1868 (1986), codified as amended at 18 U.S.C. § 3121(a).

[45] *Id.*, at 100 Stat. 1869, codified as amended at 18 U.S.C. § 3122(b)(1).

[46] Pub. L. No. 105-272, 112 Stat. 2396, 2405 (1998). The USA PATRIOT ACT, Pub. L. No. 107-56, § 214(a), 115 Stat. 286 (2001), deleted this language and substantially rewrote the FISA provisions on pen registers and trap and trace devices. The current requirement is only that "the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." 50 U.S.C. § 1842(c)(2).

The basis, however, for much of the NSA's bulk collection of metadata arises under the so-called USA PATRIOT Act.[47] That statute, which substantially amended a dozen other laws regulating the government's investigative authorities, was enacted under intense executive branch pressure in the immediate wake of 9/11. In contrast to the extensive interbranch negotiation and painstaking documentation that accompanied FISA, Congress enacted the PATRIOT Act less than two months after the September 11 attacks and without carefully crafted analysis to guide its implementation.[48]

Among the key changes that expanded the government's information gathering authority were an expansion of the definitions of "pen register" and "trap and trace" devices. ECPA previously authorized their use for telephone communications.[49] They are now defined to permit surveillance of routing information for all electronic communications, including, for example, Web surfing and email.[50]

---

[47] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 271 (2001) (hereinafter, the "USA PATRIOT Act" or "PATRIOT Act").

[48] "Legislative proposals in response to the terrorist attacks of September 11, 2001 were introduced less than a week after the attacks. President Bush signed the final bill, the USA PATRIOT Act, into law on October 26, 2001. Though the Act made significant amendments to over 15 important statutes, it was introduced with great haste and passed with little debate, and without a House, Senate, or conference report. As a result, it lacks background legislative history that often retrospectively provides necessary statutory interpretation." Electronic Privacy Information Center, *USA PATRIOT Act*, EPIC, *available at* http://epic.org/privacy/terrorism/usapatriot.

[49] Pub. L. No. 99-508, § 301(a), 100 Stat. 1871 (1986).

[50] Pub. L. No. 107-56, §§ 216(c)(2) and (3), 115 Stat. 288 (2001), codified at 18 U.S.C. § 3127. Expanding the government's authority through a mere definitional change, however, built into the law a potentially important ambiguity. Under ECPA, neither kind of device is to be used to observe "the contents of any communication." 18 U.S.C. § 3121(c). The distinction between content and routing information is readily implemented with regard to telephone communications. That distinction is far less obvious, however, for email. That is because email communications move across a variety of conduits that use routing information of different kinds. To oversimplify, an Internet Service Provider (ISP) needs only two pieces of information to route an electronic message – the IP address of the sending device and the address of the recipient server, which may belong, say, to Google, Yahoo!, or the like. The ISP does not need to consult the "header" information that indicates, for example, the actual intended recipient of the email. As far as the ISP is concerned, the "header" is content. For Google, however, the header is routing information. Google has to get its Gmail to the correct individual subscriber. Julian Sanchez, *Are Internet Backbone Pen Registers Constitutional?*, JUSTSECURITY.ORG (Sept. 23, 2013), http://justsecurity.org/2013/09/23/internet-backbone-pen-registers-constitutional. In any event, we now know from redacted FISC opinions declassified and released by the Office of the Director of National Intelligence that the FISC had to wrestle seriously with the distinction between "content," the collection of which is not permitted

Pen register authority was also extended so that its target need no longer be a foreign power or the agent of a foreign power. Under Section 214 of the Act, FISA was amended so that a pen register or trap and trace device may be sought in connection with any investigation "to protect against international terrorism or clandestine intelligence activities."[51] The only limitation regarding the use of such devices targeting United States citizens is that "such investigation of a United States person" may not be "conducted solely upon the basis of activities protected by the first amendment to the Constitution."[52]

Arguably, the most consequential change, however, appears to be the enactment of Section 215 of the Act, which authorizes the FBI Director or a designee to seek:

> an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.[53]

The application for such authority need only "specify that the records concerned are sought for an authorized investigation . . . to protect

---

through pen register or trap and trace orders, and "dialing, routing, addressing, or signaling information," which is permissible. *See* Undated Opinion by Judge John D. Bates Declassified Without Date or Caption (FISC), at 30-35, 52-54, *available at* http://www.dni.gov/files/documents/1118/CLEANEDPRTT%202.pdf (approving the re-initiation of pen register and trap and trace authority under FISA for Internet metadata). Although the opinion redacts all specifics about the precise categories of information NSA proposes to collect as metadata, we know from another declassified opinion that "information from the 'from' line of an email" is included. Undated Opinion by Judge Colleen Kollar-Kotelly Declassified Without Date or Caption (FISC), at 15, *available at* http://www.dni.gov/files/documents/1118/CLEANEDPRTT%201.pdf. For further analysis of problems lurking in the FISC's treatment of Internet metadata, *see* Julian Sanchez, *The FISC's Problematic Pen/Trap Opinion on Bulk Internet Metadata Collection*, JUSTSECURITY.ORG (Nov. 22, 2013), http://justsecurity.org/2013/11/22/fiscs-slipshod-pentrap-opinion-bulk-internet-metadata-collection.

[51] The USA PATRIOT ACT, Pub. L. No. 107-56, § 214(a), 115 Stat. 286 (2001), codified at 50 U.S.C. § 1842(c)(2).

[52] *Id.*

[53] Pub. L. No. 107-56, § 215, 115 Stat. 287 (2001), codified as amended at 50 U.S.C. § 1861(a).

against international terrorism or clandestine intelligence activities."[54] As it turns out, the Bush and Obama Administrations have relied on Section 215 to acquire telephone company records of the metadata concerning millions and millions of phone calls.[55] Because this acquisition does not entail the government's use of an electronic surveillance device, FISA does not apply.

III. THE 2005 NSA LEAKS

As expansive as these authorities may seem, it was revealed in a series of New York Times articles in 2005 that the Bush Administration, since shortly after 9/11, had been engaged in extensive warrantless wiretapping outside the FISA process.[56] The Times also revealed in general terms the existence of a broad data mining program.[57] Unlike the 1975 New York Times revelations of unlawful surveillance during the 1960s, however, the 2005 revelations prompted no comprehensive public inquiry or any establishment of a clear historical record of what happened, why, and with whose approval. It is important to take note of what we now know transpired because the further 2006 amendments to the PATRIOT Act[58] and the amendments to FISA that occurred in 2007[59] and 2008[60] were intended precisely to make lawful much of what had been of dubious legality, at best, under the Bush Administration.

---

[54] *Id.*, codified as amended at 50 U.S.C. § 1861(b)(2).

[55] Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 5, 2013), *available at* http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

[56] James Risen and Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, *available at* http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all&_r=0; Eric Lichtblau and James Risen, *Eavesdropping Effort Began Soon After Sept. 11 Attacks*, N.Y. TIMES, Dec. 18, 2005, *available at* http://query.nytimes.com/gst/fullpage.html?res=F70716F73D540C7B8DDDAB0994DD404482; James Risen and Eric Lichtblau, *Spying Program Snared U.S. Calls*, N.Y. TIMES, Dec. 21, 2005, *available at* http://www.nytimes.com/2005/12/21/politics/21nsa.html.

[57] Eric Lichtblau and James Risen, *Spy Agency Mined Vast Data Trove, Officials Report*, N.Y. TIMES, Dec. 24, 2005, *available at* http://www.nytimes.com/2005/12/24/politics/24spy.html?pagewanted=all&_r=0.

[58] *See* text at notes 97-8, *infra*.

[59] *See* text at notes 101-2, *infra*.

[60] *See* text at notes 105-8, *infra*.

The clearest, albeit still incomplete record of what we now know concerning Bush Administration surveillance and the decision making surrounding that surveillance comes from two documents. One is an "Unclassified Report on the President's Surveillance Program" released on July 10, 2009,[61] which was jointly prepared, as required by the FISA Amendments Act of 2008,[62] by the Inspectors General of Justice, Defense, the CIA, the NSA, and the Office of the Director of National Intelligence. The second is a draft March 24, 2009 report by the NSA Office of Inspector General, which was leaked by Edward Snowden.[63] Events are perhaps easiest to follow if traced with regard to particular categories of communications that NSA sought to intercept: first, the contents of telephone and Internet communications; second, telephone metadata; and third, Internet metadata. All were part of what the IG Report calls the "President's Surveillance Program" (PSP), which includes, but goes significantly beyond the Terrorist Surveillance Program revealed in the 2005 New York Times stories.

September 11, for obvious reasons, prompted NSA's interest in substantially expanding its acquisition of telephony and Internet content that might reveal foreign intelligence information. Thus, on September 14, 2001, NSA Director General Michael Hayden "approved the targeting of terrorist-associated foreign telephone numbers on communication links between the United States and foreign countries where terrorists were known to be operating."[64] At first, calls originating in the United States were collected only if communicating with specified, pre-approved numbers, but this net was expanded.[65] By September 26, because al Qaeda's leadership was in Afghanistan, General Hayden had determined that any Afghan telephone number in contact with a U.S. telephone number "was presumed to be of foreign intelligence value and could be disseminated to the FBI."[66]

---

[61] Unclassified Report on the President's Surveillance Program (July 10, 2009), *available at* https://www.fas.org/irp/eprint/psp.pdf (hereinafter 2009 Unclassified PSP Report).

[62] FISA Amendments Act of 2008, Pub. L. No. 110-261, § 301(c), 122 Stat. 2472 (2008).

[63] Office of the Inspector General, National Security Agency Central Security Service, ST-09-0002 Working Draft (Mar. 24, 2009), *available at* http://www.aclu.org/files/natsec/nsa/20130816/NSA%20IG%20Report.pdf (hereinafter NSA IG Report).

[64] *Id.* at 3.

[65] *Id.*

[66] *Id.*

During this period, General Hayden was apparently in discussions with CIA Director George Tenet and the White House about the feared inadequacy of existing legal authorities to permit the kinds of expanded acquisition that could be useful in the wake of September 11.[67] As a consequence, President Bush, on October 4, 2011, issued a secret memorandum entitled, "Authorization for Specified Electronic Surveillance Activities During a Limited Period to Detect and Prevent Acts of Terrorism Within the United States."[68] As summarized in the Draft NSA IG Report, under the President's order:

> NSA could collect the content and associated metadata of telephony and Internet communications for which there was probable cause to believe that one of the communicants was in Afghanistan or that one. communicant was engaged in or preparing for acts of international terrorism. In addition, NSA was authorized to acquire telephony and Internet metadata for communications with at least one communicant outside the United States or for which no communicant was known to be a citizen of the United States. NSA was also allowed to retain, process, analyze and disseminate intelligence from the communications acquired under the authority.[69]

This authorization was subsequently modified from time-to-time depending, one presumes, on the White House's assessment of the scope of national security needs.[70]

With regard to both telephony and Internet content, the acquisition permitted by the Bush order went beyond FISA in a number of respects. For example, certain communications originating or received in the United States might be intercepted without warrant even though they were unambiguously covered by the FISA definition of "electronic surveillance."[71] The NSA could collect in the United States Internet content for foreign communications that simply

---

[67] *Id.* at 4, 6-7.

[68] *Id.* at 1.

[69] *Id.* at 8.

[70] *Id.*

[71] *See* text at notes 37-40, *supra*.

"transited" U.S. electronic networks;[72] thus, communications between foreign nationals might be intercepted in the United States if they were using an email service that resides on U.S. territory, even if the interception also captured content involving U.S. "communicants" having a reasonable expectation of privacy.

After the warrantless surveillance of electronic communications content was divulged in The New York Times, President Bush acknowledged in a December 17, 2005 radio address what the Administration called the Terrorist Surveillance Program (TSP).[73] In addition, the Administration prepared two public presentations of its legal position. The more extensive of these was a January 19, 2006 Justice Department memorandum of unattributed authorship, entitled, "Legal Authorities Supporting the Activities of the National Security Agency Described by the President."[74] In this memorandum,

---

[72] FISA encompasses as "electronic surveillance": "the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes." 50 U.S.C. § 1801(f)(4). Internet traffic does not count as "wire . . . communication" because FISA defines "wire communication" as "any communication while it is being carried by a wire, cable, or other like connection furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications." 50 U.S.C. § 1801(l). Because Internet service providers do not operate as "common carriers" in the provision of Internet service, the installation of an interception device in the United States for acquiring information from Internet providers that captures information that would be protected by the Fourth Amendment from warrantless seizure, is covered by this definition.

This is not the only respect in which the NSA was likely concerned that FISA had not kept up with technological change in the global communications system. Consider, for example, the migration of foreign and trans-border communications from satellite transmission (where they could be plucked out of the air by NSA without implicating FISA) to undersea fiber optic cables (on which communications potentially implicate FISA). On the history of tapping such cables, *see* Olga Khazan, *The Creepy, Long-Standing Practice of Undersea Cable Tapping*, THEATLANTIC.COM (July 16, 2013), http://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855.

[73] President George W. Bush, "President's Radio Address," 2005 WL 3450560 (Dec. 17, 2005), summarized in JEFFREY W. SEIFERT, CONGRESSIONAL RESEACH SERVICE, DATA MINING AND HOMELAND SECURITY: AN OVERVIEW 23-24 (2007), *available at* http://www.fas.org/sgp/crs/homesec/RL31798.pdf.

[74] U.S. Department of Justice, Legal Authorities Supporting the Activities of the National Security Agency Described by the President (Jan. 19, 2006), *reprinted in* David Cole and Martin S. Lederman, *The National Security Agency's Domestic Spying Program: Framing the Debate*, 81 IND. L. REV. 1355, 1374 (2006) (hereinafter, "NSA Legal Authorities").

as in an earlier letter from Assistant Attorney General William Moscella to the leadership of the House and Senate Select Committees on Intelligence,[75] the Administration's legal stance rested to two essential propositions. The first is that warrantless electronic surveillance directed at al Qaeda and its supporters fell within the President's inherent war powers, as confirmed by the Authorization to Use Military Force in Afghanistan, or the AUMF,[76] enacted by Congress on September 12, 2001.[77] The second was that the President has inherent constitutional power to conduct the TSP no matter what the AUMF says, and, if FISA is read to preclude this particular program of foreign intelligence surveillance, then FISA is unconstitutional.[78]

Although both propositions were highly problematic–the Office of Legal Counsel subsequently repudiated several aspects of its earlier legal memoranda that were the basis of this legal defense[79]–one could imagine at least a coherent argument on behalf of programs limited to targeting communications to and from persons reasonably believed to be acting in Afghanistan or on behalf of al Qaeda. That defense, however, would be yet more dubious if extended to the NSA's metadata programs, which clearly and foreseeably reached millions of communications with no Afghanistan or al Qaeda connection. Although the New York Times stories, among others, did indicate in 2005 some sort of undisclosed NSA data mining program,[80] the Bush

---

[75] Letter from William E. Moschella, Assistant Attorney General, Office of Legal Affairs, U.S. Department of Justice to the Leadership of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence (Dec. 22, 2005), reprinted in Cole and Lederman, *supra* note 75, at 1360.

[76] Pub. L. No. 107-40, 15 Stat. 224 (2001) (hereinafter, "AUMF").

[77] NSA Legal Authorities, *supra* note 75, at 1379-90.

[78] *Id.* at 1407.

[79] Memorandum for the Files by Steven G. Bradbury, Principal Deputy Assistant Attorney General, Office of Legal Counsel re: Status of Certain OLC Opinions Issued in the Aftermath of the Terrorist Attacks of September 11, 2001 (Jan. 15, 2009), *available at* http://www.justice.gov/opa/documents/memostatusolcopinions01152009.pdf; *see also* PETER M. SHANE AND HAROLD H. BRUFF, SEPARATION OF POWERS LAW: CASES AND MATERIALS 718-719 (3d ed. 2011).

[80] Eric Lichtblau and James Risen, *supra* note 58.

Administration's disclosures did not address its collection of metadata.[81]

The collection of telephony metadata gave the NSA information regarding the originating numbers and numbers called, as well as call duration, for apparently every telephone call made over the networks of cooperating telephone companies.[82] No requirement was imposed that limitations were imposed regarding the location of callers or participation of non-U.S. persons because the NSA did not acquire this information through government electronic surveillance.[83] This information is regularly collected by telephone companies for their own business purposes and was requested pursuant to the PATRIOT Act Section 215's authority for the acquisition of "tangible things," namely, business records.[84] As reported by the IG: "NSA determined that under the [2011 Presidential] Authorization it could gain access to approximately 81% of the international calls into and out of the United States through three corporate partners."[85]

Such metadata were then available to the NSA for what it called "contact chaining." As explained in the IG Report: "Contact chaining is the process of building a network graph that models the communication (e-mail, telephony, etc.) patterns of targeted entities (people, organizations, etc.) and their associates from the communications sent or received by the targets."[86] Furthermore:

> Additional chaining can be performed on the associates' contacts to determine patterns in the way a

---

[81] An electronic search of the Bush Administration's documents discussing the Terrorist Surveillance Program, cited in notes 75 and 76, *supra*, confirms that neither documents use the words "metadata" or "Internet."

[82] Administration White Paper: Bulk Collection of Telephony Metadata Under Section 215 of the USA PATRIOT Act, at 3 (Aug. 9, 2013), *available at* http://big.assets.huffingtonpost.com/Section215.pdf.

[83] *See, e.g.*, In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted], BR-1380, at 4 (FISC, Apr. 25, 2013) (ordering respondent to produce "all call detail records or 'telephony metadata' created by-for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls."), *available at* http://www.fas.org/irp/news/2013/07/215_order.pdf.

[84] Pub. L. No.107-56, § 215, 115 Stat. 287 (2001), codified as amended at 50 U.S.C. § 1861(a).

[85] NSA IG Report, *supra* note 64, at 27.

[86] *Id.* at 13.

> network of targets may communicate. Additional degrees of separation from the initial target are referred to as "hops." For example a direct contact is one hop away from the target. A contact of the direct contact would be described as being 2 hops away from the target. The resulting contact-graph is subsequently analyzed for intelligence and to develop potential investigative leads.[87]

Analysts would do contact chaining on the U.S. numbers to determine, for example, which numbers were linked to foreign numbers. As the IG recounts: "The records were used by NSA Counter-Terrorism metadata analysts to perform call chaining and network reconstruction between known al Qaeda and al Qaeda-affiliate telephone numbers and previously unknown telephone numbers with which they had been in contact."[88]

Until March, 2004, telephone companies were also providing the NSA metadata concerning Internet communications.[89] In March, 2004, however, the Justice Department's Office of Legal Counsel, under new leadership, determined that the collection of Internet metadata could not be squared with either FISA or the PATRIOT Act.[90] Although no memorandum of its advice has been made public, two propositions probably led to this conclusion.[91] First, because Internet metadata are not routinely kept by the cooperating companies, its acquisition would not fit under Section 215; collecting the metadata would amount to electronic surveillance. Second, because there was likely no way to exclude the collection of metadata regarding millions of emails from U.S. communicants, their bulk acquisition plainly violated the terms of FISA. In a much-publicized and dramatic episode, Attorney General Ashcroft, lying in a hospital bed, refused to sign off on President Bush's March 11, 2004

---

[87] *Id.* at 13 n. 6.

[88] *Id.* at 33.

[89] *Id.* at 8, 32, 38.

[90] *Id.* at 38.

[91] Julian Sanchez, *What the Ashcroft "Hospital Showdown" on NSA spying was all about: How the government sought to justify blanket collection of Internet metadata*, ARSTECHNICA.COM (July 29 2013), http://arstechnica.com/tech-policy/2013/07/what-the-ashcroft-hospital-showdown-on-nsa-spying-was-all-about.

authorization for Internet metadata collection.[92] The NSA initially continued the interception anyway, based on approval by White House Counsel, rather than the Attorney General.[93] On March 26, 2004, however, President Bush temporarily discontinued the authorization for bulk Internet metadata collection.[94]

IV. PATRIOT ACT AMENDMENTS OF 2006, THE PROTECT AMERICA ACT AND THE FISA AMENDMENTS OF 1978

As noted above, President Bush's acknowledgement of NSA warrantless content collection programs did not precipitate anything like the extended public discussion and systematic congressional investigations that preceded the enactment of FISA–or that is occurring now in the wake of the Snowden leaks. Instead, the Administration proceeded to consult with the Foreign Intelligence Surveillance Court to develop rationales under which programs first developed under President Bush's 2001 order could be legitimated instead by orders of the FISC.

The first of these transitions actually occurred with regard to the Internet metadata program that had been suspended in March, 2004. By July, 2004, the Administration was able to secure from the FISC a "pen register/trap and trace" order to permit the Internet metadata collection: "[T]he order essentially gave NSA the same authority to collect bulk Internet metadata that it had under the PSP, except that it specified the datalinks from which NSA could collect, and it limited the number of people that could access the data."[95]

---

[92] Daniel Klaidman, Stuart Taylor Jr. & Evan Thomas, *Palace Revolt,* NEWSWEEK, Feb. 6, 2006, at 34. Although the Newsweek article was the first to reveal the fact of a hospital pilgrimage, its full details later emerged through testimony by former Deputy Attorney General Comey to the Senate Judiciary Committee. Testimony of James B. Comey, Former Deputy Attorney General, U.S. Department of Justice to the Committee on the Judiciary, *Hearing on Preserving Prosecutorial Independence: Is the Department of Justice Politicizing the Hiring and Firing of U.S. Attorneys? – Part IV*, U.S. Senate, 110th Cong., 1st Sess. (2006), *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/05/15/AR2007051501043.html.

[93] NSA IG Report, *supra* note 64, at 38.

[94] *Id.* at 32.

[95] *Id.* at 39. Although released in a form that redacted the date of issuance, the Undated Opinion by Judge Colleen Kollar-Kotelly Declassified Without Date or Caption (FISC), *available at* http://www.dni.gov/files/documents/1118/CLEANEDPRTT%201.pdf, reads as if it represents the original order. There are arguably three quite uncomfortable features of Judge Kollar-Kotelly's analysis. First, the pen register/trap and trace provisions of FISA, speak of applications to authorize "*a* pen register or trap and trace device," § 50 U.S.C. 1842(a)(1) (emphasis added), which might well suggest that Congress did not intend to

As for telephony metadata, NSA acquisition was pursued under PATRIOT Act Section 215. On March 9, 2006, Congress enacted the "USA PATRIOT Improvement and Reauthorization Act of 2005," which amended Section 215 to require only that the "records [pursued under that section] are sought for an authorized investigation . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities."[96] A FISC Order covering telephone metadata was instituted in May, 2006, producing no reduction in metadata acquisition, limiting only who could access the data and requiring somewhat more stringent oversight.[97]

The orders covering telephone and Internet content proved more complex because of the large volume of telephone numbers and email addresses–"selectors," in NSA parlance–that the NSA wanted to include. With regard to foreign "selectors," the NSA and Justice attempted to solve this problem in 2007 by changing "the traditional FISA definition of a 'facility' [to be targeted] as a specific telephone number or email address . . . to encompass the gateway or cable head that foreign targets use for communications."[98] Even this move, however, significantly reduced the number of target addresses available to the NSA. The documentation that the FISC demanded to justify the inclusion of specific selectors reduced the

---

authorize FISA to permit bulk acquisition of Internet (or any other) metadata under a single FISC order covering multiple devices. Second, although the court acknowledges that the vast majority of captured metadata will not be related to terrorism or foreign intelligence, *id.* at 48, Judge Kollar-Kotelly finds that the information sought is "relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities," as FISA requires, § 50 U.S.C. 1842(c)(2), apparently because the metadata search is not too broad to satisfy the Fourth Amendment's reasonableness requirements – a seeming non sequitur. *Id.* at 50. Finally, the judge's order contains a series of requirements for the storage, accessing and dissemination of the acquired metadata, even though § 50 U.S.C. 1842 makes no provision for the judicial imposition of such conditions. Orin Kerr, *Problems with the FISC's Newly-Declassified Opinion on Bulk Collection of Internet Metadata*, LAWFARE (Nov. 19, 2013), http://www.lawfareblog.com/2013/11/problems-with-the-fiscs-newly-declassified-opinion-on-bulk-collection-of-internet-metadata.

[96] Pub. L. No.107-56, § 215, 115 Stat. 287 (2001), codified as amended at 50 U.S.C. § 1861.

[97] *In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted], BR06-05 (FISC, May 24, 2006), *available at* https://www.aclu.org/files/assets/pub_May%2024%202006%20Order%20from%20FISC.pdf.

[98] NSA IG Report, *supra* note 64, at 41.

number of foreign addresses available from 11,000 to 3,000 and the number of domestic addresses to essentially just one.[99]

The unworkability of the FISC orders, especially for content, led the Administration in 2007 to seek amendments to FISA. Congress's initial, short-term solution was the Protect America Act of 2007.[100] The PAA:

> authorized the Director of National Intelligence and the Attorney General to acquire foreign intelligence information concerning persons outside the United States for one year, if the acquisition involved the assistance of a communication service provider, custodian or other person, and a significant purpose of the collection was the acquisition of foreign intelligence information. The Act was set to sunset after 180 days, on February 1, 2008.[101]

The PAA was highly controversial in a number of respects. For those skeptical of the TSP, the Act seemed to go too far in relaxing judicial oversight of electronic surveillance and creating loopholes through which warrantless surveillance might be directed at persons within the United States.[102]

Congress ultimately replaced the PAA with the Foreign Intelligence Surveillance Act of 1978 Amendments of 2008.[103] The Amendments accomplished a number of key things. Among its more controversial sections, it provided a path to immunity from liability for telecommunications companies that may have violated FISA by cooperating with Bush Administration surveillance programs between 2001 and 2007.[104] Even more important for the future, however, Section 702 of the Amendments added a new title to FISA providing

---

[99] *Id.* at 41-42.

[100] Pub. L. No. 110-55, 121 Stat. 7 (2007).

[101] S. REP.110-209 at 6 (2007).

[102] *See, e.g., ACLU Fact Sheet on the "Police America Act,"* ACLU.ORG (Aug. 7, 2007), https://www.aclu.org/national-security/aclu-fact-sheet-%E2%80%9Cpolice-america-act.

[103] Pub. L. No. 110-261, 122 Stat. 2436 (2008).

[104] *Id.* at Title II, 122 Stat. 2467, codified at 50 U.S.C. §§ 1885a-1885c. For analysis, *see* Edward C. Liu, Retroactive Immunity Provided by the FISA Amendments Act of 2008 (Congressional Research Service, July 25, 2008), *available at* http://www.fas.org/sgp/crs/intel/RL34600.pdf.

so-called, "Additional Procedures for Targeting Communications of Certain Persons Outside the United States,"[105] which were to remain in effect until December 31, 2012, but which have since been extended.[106] When a targeted individual is reasonably believed to be outside the United States, the Attorney General may apply for an order approving the acquisition from that person of foreign intelligence information under conditions slightly more relaxed than those specified by 50 U.S.C. §§ 1804 and 1805. For example, if the targeted person is "an officer or employee" of a foreign power, they need not themselves be a "foreign power," or an "agent of a foreign power."[107] Alternatively, when a targeted person is reasonably believed to be outside the United States, but the Attorney General wishes to conduct electronic surveillance of the target, or to acquire the target's stored electronic data or communications, within the United States, the Attorney General may seek an order from the FISC that not only approves the acquisition in question, but compels the cooperation of private "electronic communication service providers" in the acquisition.[108]

The most dramatic new procedures, however, categorically allow the Attorney General and the Director of National Intelligence to institute legally authorized programs of surveillance of up to one year "of persons reasonably believed to be located outside the United States."[109] Such programs do not require that targeted individuals be named to the FISC, but only that the Attorney General and the DNI certify that procedures are in place that are reasonably designed to limit surveillance to persons in general who are reasonably believed to be outside the United States, and that would prevent the intentional acquisition of communications among persons all of whom are known to be inside the United States.[110] It is required also that minimization procedures be in place[111] and that "a significant purpose" of the

---

[105] *Id.* Title I, at 122 Stat. 2437 (2008), codified at 50 U.S.C. §§ 1881-1881g.

[106] Foreign Intelligence Surveillance Act (FISA) Amendments Act Reauthorization Act of 2012, Pub. L. No. 112-238, 126 Stat. 1631 (2008).

[107] 50 U.S.C. § 1881c.

[108] 50 U.S.C. § 1881b.

[109] 50 U.S.C. § 1881a.

[110] 50 U.S.C. § 1881a(g).

[111] 50 U.S.C. § 1881a(e)(1).

acquisition be obtaining foreign intelligence information.[112] The Attorney General and DNI may jointly initiate such acquisitions even without judicial certification if they jointly determine "that exigent circumstances exist because, without immediate implementation of an authorization. . . intelligence important to the national security of the United States may be lost or not timely acquired and time does not permit the issuance" of a judicial order.[113] These procedures essentially eliminate the documentation complexities that made the FISC's 2007 orders on content acquisition impracticable from NSA's point of view. The new Section 702 also appears to eliminate the statutory barrier to the collection of Internet metadata. Yet the Obama Administration reportedly shut down the program, for unspecified reasons, in 2011.[114]

V. THE SNOWDEN REVELATIONS ABOUT INFORMATION COLLECTION AND STATUTORY UNCERTAINTY: SEGUE TO A SYMPOSIUM

On June 5, 2013, The Guardian published the first of a stream of explosive news stories about NSA surveillance based on documents leaked by Edward Snowden, an employee of NSA contractor Booz Allen Hamilton.[115] The first document to be disclosed was a secret FISC order compelling a Verizon subsidiary to turn over call details for every domestic and international phone call placed on its network during a three-month period.[116] The order made clear for the first time that the NSA was tracking metadata on the telephone communications of millions of Americans, not just suspected agents of a foreign power or terrorists.

---

[112] 50 U.S.C. § 1881a(g)(2)(v).

[113] 50 U.S.C. § 1881a(c)(2).

[114] Glenn Greenwald and Spencer Ackerman, *NSA Collected US Email Records in Bulk for More Than Two Years Under Obama*, THE GUARDIAN (June 27, 2013), *available at* http://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama.

[115] Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 5, 2013), *available at* http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

[116] *In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from Verizon Business Network Services, Inc. on BEHALF of MCI Communication Services, Inc. D/B/A Verizon Business Services, BR-13-80 (FISC, Apr. 25, 2013), *available at* https://www.aclu.org/files/natsec/nsa/20130816/Section%20215%20-%20Secondary%20Order%20-%20Verizon.pdf.

A story published the next day revealed the existence of a computer system called PRISM, which–according to a set of leaked training slides–allows the Government to analyze information it collects from Microsoft, Google, Yahoo!, Facebook, PalTalk, YouTube, Skype, AOL, and Apple.[117] This material includes "search history, the content of emails, file transfers and live chats."[118]

The disclosure of these two programs involving the massive collection of both telephony metadata and online communications set the stage for what has been an extraordinary string of disclosures[119]–some in the press, some through government declassification–that have shed unprecedented light on the workings of our foreign intelligence surveillance regime. Among the document leaks are:

- NSA documents describing its "mission capabilities" based on the collection of metadata;
- FISC documents concerning NSA targeting and minimization procedures;
- Justice Department briefings to congressional committees concerning the nature of NSA collection programs;
- NSA documents concerning programs for collecting Internet and telephony data from fiber-optic cable networks;
- NSA documents on strategies to defeat encryption; and

---

[117] Glenn Greenwald and Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, THE GUARDIAN (June 6, 2013), *available at* http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

[118] PRISM/US-984XN Overview OR The SJGAD Used Most in NSA Reporting – Overview, Slide 3, *available at* https://www.aclu.org/files/natsec/nsa/20130816/PRISM%20Overview%20Powerpoint%20Slides.pdf.

[119] My summaries of the kinds of documents either leaked or declassified is derived from the ACLU's online library of *NSA Documents Released to the Public Since June 2013*, ACLU.ORG, https://www.aclu.org/nsa-documents-released-public-june-2013. Summaries of key documents may also be found on LAWFARE, http://www.lawfareblog.com.

- NSA documents revealing compliance problems in the implementation of collection programs subject to FISC orders.

For its part, the Government has produced or released declassified versions of an even larger number of documents. These include:

- correspondence with and testimony to Congress concerning the programs at issue, reflecting the system of congressional oversight;

- an Administration white paper on the bulk collection of telephony metadata under Section 215 of the PATRIOT Act;

- FISC opinions reviewing the NSA's bulk data collection programs; and

- reports on the NSA's compliance with the FISC's Section 702 guidelines and minimization procedures;

Even in severely redacted form, the FISC opinions are especially intriguing. They display a court typically deferential to the Justice Department's statutory and constitutional arguments, but intensely engaged in the crafting and monitoring of the targeting and minimization requirements the court imposes under FISA. We learn that, at least in one instance, the court found aspects of the NSA's "upstream collection" of Internet transactions including multiple communications to be unlawful.[120]

Unsurprisingly given the magnitude of the programs now under scrutiny, the public's incomplete access to the assessments that drive these programs, and the extraordinary density of the documents to which we now have access, reactions to the Snowden revelations have differed markedly. Benjamin Wittes, a Brookings Institution senior fellow and editor-in-chief of the exceptional Lawfare blog, has written a generally sanguine assessment:

> [N]othing in the current disclosures should cause us to lose faith in the essential integrity of the post-

[120] [Redacted Caption], at 67-79 (FISC, Oct. 3, 2011), *available at* https://www.aclu.org/files/assets/fisc_opinion_10.3.2011.pdf.

> Watergate system of delegated intelligence oversight. To the contrary, those disclosures should give the public great confidence both in the oversight mechanisms within the executive branch and in the judicial oversight mechanisms that review both the Section 215 collection program and the Section 702 collection program.
>
> The disclosures show no evidence of any intentional, unlawful spying on Americans or abuses of civil liberties. They show a low rate of the sort of errors any complex system of technical collection will inevitably yield. They show robust compliance procedures. They show earnest and serious efforts to keep the Congress informed—including members not on this committee or its counterpart in the House of Representatives. And they show an ongoing dialogue with the Foreign Intelligence Surveillance Court (FISC) about the parameters of the agency's legal authorities and a commitment both to keeping the court informed of activities and to complying with its judgments as to their legality. The FISC, meanwhile, in these documents looks nothing like the rubber stamp that it is portrayed to be in countless caricatures. It looks, rather, like a judicial institution of considerable energy, one whose oversight role with respect to both Section 215 and Section 702 requires enormous time and energy on the part of the executive to satisfy.[121]

It is not hard to find less positive views. Jennifer Granick, director of civil liberties at the Stanford Center for Internet and Society and law professor Christopher Jon Sprigman, describe the NSA surveillance program as "criminal":

> The [NSA's bulk data] programs violate both the letter and the spirit of federal law. No statute explicitly authorizes mass surveillance. Through a series of legal

---

[121] Prepared Statement of Benjamin Wittes Senior Fellow at the Brookings Institution before the Senate Select Committee on Intelligence, *Legislative Changes to the Foreign Intelligence Surveillance Act* (Sept. 26, 2013), at 2-3, *available at* http://www.lawfareblog.com/wp-content/uploads/2013/09/Wittes-SSCI-Hearing-Statement_Final-Draft_9.26.13.pdf.

> contortions, the Obama administration has argued that Congress, since 9/11, intended to implicitly authorize mass surveillance. But this strategy mostly consists of wordplay, fear-mongering and a highly selective reading of the law.[122]

Law professor Martin Lederman, a former Obama Justice Department official, offers a mixed assessment of the FISC:

> The disclosures . . . have demonstrated, I think, that the FISC is extremely resolute, and careful, about ensuring that the NSA and FBI comply with the terms of the FISC's own orders, including the so-called "minimization" requirements–in part because the lawyers in . . . DOJ's National Security Division, take very seriously their responsibility to bring to the court's attention any compliance problems. When it comes to the more fundamental legal questions about the proper statutory and constitutional scope of a proposed program, however, the FISC process is not nearly as thorough or reliable, in large measure because the court hears from only one side.[123]

The aim of this symposium is to advance our national assessment of the NSA by looking at four key questions: the programs' legality, their contribution to national security, their impact on civil liberties, and possible avenues for constructive change. Professor John Yoo, whose defense of the Bush Administration surveillance programs proved controversial,[124] concludes that the programs revealed by the

---

[122] Jennifer Stisa Granick and Christopher Jon Sprigman, *The Criminal N.S.A.*, N.Y. TIMES (June 27, 2013), *available at* http://www.nytimes.com/2013/06/28/opinion/the-criminal-nsa.html?_r=0.

[123] Marty Lederman, *The Kris Paper, and the Problematic FISC Opinion on the Section 215 "Metadata" Collection Program*, JUST SECURITY (Oct. 1, 2013, updated Oct. 14, 2013), *available at* http://justsecurity.org/2013/10/01/kris-paper-legality-section-215-metadata-collection.

[124] The 2009 Unclassified PSP Report, *supra* note 62, criticizes Professor Yoo's legal opinions for giving insufficient weight to several provisions of FISA that would have appeared problematic for his conclusions, for failing to discuss *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579 (1952), as it might bear on his analysis, and for inaccuracies in his memos' descriptions of the activities being reviewed. *Id.* at 10-14. It perhaps ought to be said, especially in the context of this symposium, that the constitutional analysis undergirding Professor Yoo's confidential professional advice is fully revealed in his

Snowdon leaks are both constitutional and statutorily authorized.[125] Specifically, he finds that the metadata records acquired under Section 215 are "tangible things . . . relevant to an authorized investigation (other than a threat assessment) conducted in accordance with subsection (a)(2) to . . . protect against international terrorism," and thus clearly within purview of the statute.[126] The content collection programs under Section 702, because they target non-U.S. persons believed to be outside the U.S., likewise fall within the bounds of explicit statutory authority.[127]

Of the two statutory arguments, the Section 215 argument is clearly the more vulnerable–despite its acceptance by the FISC. As others have noted, "most of the information collected does not relate to individuals suspected of any wrongdoing."[128] The metadata can be viewed as relevant only under a needle-in-the-haystack theory–namely, that the likely existence of some modicum of specifically relevant data in the bulk collection makes all the records relevant because, at the moment of collection, it is impossible to be any more specific about what that modicum may be. This would seem to eliminate entirely the distinction between relevant and irrelevant records.[129]

Also, the use of Section 215 to elicit bulk metadata from telecommunications companies seems to run afoul of the strict statutory limits on the permissible disclosure to the government of telecommunication subscriber records.[130] 18 U.S.C. §2702(a) forbids

---

academic writings both before and after his period of government service; he does not shy away from exposing his views to public critique.

[125] John Yoo, *The Legality of the National Security Agency's Bulk Data Surveillance Programs*, 10 ISJLP 324-326 (2014).

[126] *Id.* at 305.

[127] *Id.* at 311-313.

[128] Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, at 50 (2013), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2344774.

[129] For a detailed critical analysis of the Government's Section 215 argument, see *id.* at 48-64. For a comprehensive review of the interpretive issues raised under Section 215, see David S. Kris, *On the Bulk Collection of Tangible Things*, 1 LAWFARE RES. PAPER SERIES No. 4 (2013), *available at* http://www.lawfareblog.com/wp-content/uploads/2013/09/Lawfare-Research-Paper-Series-No.-4-2.pdf. The Administration's official defense of its position appears as Administration White Paper: Bulk Collection of Telephony Metadata Under Section 215 of the USA PATRIOT Act, at 3 (Aug. 9, 2013), *available at* http://big.assets.huffingtonpost.com/Section215.pdf.

[130] Donohue, *supra* note 129, at 63-64; Lederman, *supra* note 124.

"a provider of remote computing service or electronic communication service to the public [to] knowingly divulge a record or other information pertaining to a subscriber to or customer of such service . . . to any governmental entity." Section 2702(c) includes a number of exemptions to this prohibition, but none covers the blanket provision of business records.[131] The prohibition in §2702(a) was added by § 212(a)(1)(B) of the PATRIOT Act, the same statute that created the Section 215 "tangible things" authority.[132] The omission of a Section 215 exception to the Section 212 prohibition hardly seems like an oversight.[133]

---

[131] A provider described in subsection (a) may divulge the contents of a communication—

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

(2) as otherwise authorized in section 2517, 2511 (2)(a), or 2703 of this title;

(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A;

(7) to a law enforcement agency—

(A) if the contents—

(i) were inadvertently obtained by the service provider; and

(ii) appear to pertain to the commission of a crime; or

[(B) Repealed. Pub. L. 108–21, title V, § 508(b)(1)(A),Apr. 30, 2003, 117 Stat. 684]

(8) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.

18 U.S.C. § 2702(c).

[132] Pub. L. No. 107-56, 115 Stat. 272, 284 (2001).

[133] The FISC's handling of this issue seems flatly to ignore the plain statutory language. In re Production of Tangible Things From [REDACTED], Supplemental Opinion, BR 08-13, at 3 (FISC, Mar. 2, 2009), *available at*

Much of the consternation bestirred by this statutory uncertainty has been devoted to the degree that the FISC's acquiescence in the Administration's arguments on behalf of Section 215 authority may reveal the weakness of a system of judicial oversight in which the surveillance target or his or her advocate never appear.[134] Targets become aware of their surveillance–and able to challenge it–only if subsequent criminal prosecution occurs and the government reveals the surveillance as a source of evidence against the defendant.[135] The possibility that the Government has systematically violated Congress's precise delimitation of its bulk acquisition authority has perhaps stirred less outrage than it otherwise might on the assumption that–with the Snowden revelations now before us–Congress will eventually determine yet more definitively whether bulk metadata collection of the kind so far undertaken should or should not be lawful.

The prospects for legislative reform, however, are presumably contingent also on the kinds of surveillance that the Constitution permits. Professor Yoo argues that the programs so far revealed pass Fourth Amendment muster either because the information acquired or the targets of investigation are beyond Fourth Amendment protection, and the searches embodied in these programs pass the test of reasonableness.[136] Like the Administration, Professor Yoo relies, in

---

http://www.dni.gov/files/documents/section/pub_Dec%2012%202008%20Supplemental%20Opinions%20from%20the%20FISC.pdf. As summarized by Professor Lederman: "Judge Walton's analysis relied entirely on the fact that, under one of the exceptions to section 2702(c), the FBI can issue a 'national security letter' (NSL) to an electronic communications service provider, requesting that it disclose a customer's call records, without the approval or involvement of the FISC." *See* 18 U.S.C. § 2709. Judge Walton reasoned that it "would have been 'anomalous' for Congress to permit the Bureau to obtain such records from providers with a simple letter signed by an FBI official, but to have prohibited the FBI from obtaining the same metadata with FISC approval and the oversight and minimization requirements prescribed by section 215." Lederman, *supra* note 124. The obvious problem with this analysis, as both Professors Lederman and Donohue note, Donohue, *supra* note 129, at 63-64, is that, however "anomalous" the statutory language may be, Judge Walton's analysis adds an additional exception to 18 U.S.C. § 2702(c) that flies in the face of its terms and is nowhere supported by legislative history.

[134] *See* Lederman, *supra* note 124.

[135] The Justice Department is currently conducting a review of all criminal cases in which the government has used evidence gathered pursuant to FISA and may be notifying defendants in some of those cases that they were subjected to warrantless surveillance. Sari Horwitz, *Justice Is Reviewing Criminal Cases That Used Surveillance Evidence Gathered Under FISA*, WASH. POST (Nov. 15, 2013), *available at* http://www.washingtonpost.com/world/national-security/justice-reviewing-criminal-cases-that-used-evidence-gathered-under-fisa-act/2013/11/15/0aea6420-4e0d-11e3-9890-a1e0997fb0c0_story.html.

[136] Yoo, *supra* note 3, at 301-326.

his Fourth Amendment defense of the metadata collection, on *Smith v. Maryland*,[137] which held that the government did not need a warrant to track phone numbers because, in using telephone networks, callers voluntarily disclosed their numbers to a third party–namely, the phone company–thus eliminating the expectation of privacy. If *Smith* is fully applicable to the Section 215 orders, the Fourth Amendment issue does seem to have been decided in the Government's favor. Commentators who dissent rely chiefly on the concurring opinions of five Justices in the Supreme Court's recent decision forbidding the warrantless attachment of GPS tracking devices on private automobiles which indicated their openness to rethinking whether *Smith* ought to apply to searches for aggregate data.[138] So far, however, the Government's Fourth Amendment case seems plausibly grounded in precedent.

Professor Katherine Strandburg argues, however, that the programs Snowden revealed violate constitutional rights in other respects. Specifically, *Membership Lists, Metadata, and Freedom of Association's Specificity Requirement*[139] argues that metadata surveillance is unconstitutional unless conducted in compliance with the First Amendment's guarantee of freedom of association. As analyzed by Professor Strandburg, that right entails certain specificity requirements that the current Section 215 programs do not meet.

For many Americans, the wisdom or imprudence of the NSA programs will depend less on legal argument and more on what NSA surveillance contributes to or detracts from national security and civil liberties. Mark D. Young, who served as a Senior Advisor in the United States Cyber Command Directorate for Plans and Policy–and who was formerly Special Counsel for Defense Intelligence for the House Permanent Select Committee on Intelligence–argues that the Snowden leaks have compromised U.S. national security in four areas: facilitating operational adjustments in the techniques and security practices of our adversaries; complicating U.S. foreign relations; impairing important cooperation between the U.S. government and private industry; and unjustifiably reducing public confidence in the National Security Agency, with likely negative impacts on its resources and authorities.[140] Although his essay does not attempt to detail the

---

[137] 442 US 735 (1979).

[138] United States v. Jones, 132 S.Ct. 945, 954 (2012) (Sotomayor, J., concurring); *id.* at 957 (Alito, J., concurring).

[139] 10 ISJLP 327-365 (2014).

[140] Mark D. Young, *National Insecurity: The Impacts of Illegal Disclosures of Classified Information*, 10 ISJLP 367-406 (2014).

specific ways in which NSA surveillance has been valuable for protecting national security, he credits the positive representations in this regard of those most closely involved with NSA's programs, as well as what he takes to be their underlying logic.

For their part, however, political scientist John Mueller and engineer Mark G. Stewart seriously question both the need for secrecy and whether the metadata program, in particular, is truly justified on a national security basis.[141] Their review of the program's claimed successes lead them to conclude that the program "would very likely fail a full cost-benefit analysis handily even without taking into consideration privacy and civil liberties concerns."[142]

The debate over civil liberties might well seem one-sided–surveillance would not seem to offer any immediate civil liberties advantages–although proponents of NSA surveillance may assert that surveillance serves the cause of civil liberties in an indirect, but important way. It could be argued, if the programs help the government to fend off terrorist attack, they necessarily help to promote an atmosphere of public calm that is more conducive to respect for civil liberties. Speaking of even the limited oversight provided by the FISC, David Addington, Vice President Cheney's Chief of Staff, predicted: "We're just one bomb away from getting rid of that obnoxious court."[143] Even though Mr. Addington's words may have created what one hopes is the inadvertent impression that he would have welcomed that attack, our history after 9/11 reinforces the fundamental point that the public is more vigilant about its civil liberties when it feels safe. The argument, in short, is that without security, there is no liberty.

For civil libertarians, however, any such argument is quite likely to pale given the more direct civil liberties impacts of mass surveillance. In *NSA Surveillance: The Implications for Civil Liberties*, Shayana Kadidal, the senior managing attorney of the Guantánamo Global Justice Initiative at the Center for Constitutional Rights in New York City, asserts that such programs threaten the very independence of citizen thought and action that are central to democratic governance.[144] He illustrates that idea concretely by explaining the

---

[141] John Mueller and Mark G. Stewart, *Secret without Reason and Costly without Accomplishment: Questioning the NSA's Metadata Program*, 10 ISJLP 407-432 (2014).

[142] *Id.* at 430-431.

[143] JACK GOLDSMITH, THE TERROR PRESIDENCY: LAW AND JUDGMENT INSIDE THE BUSH ADMINISTRATION 181 (2007).

[144] 10 ISJLP 433-479 (2014).

impact of the NSA programs on his own work and on the work of other lawyers who represent politically unpopular or vulnerable clients. Like Professors Mueller and Stewart, he also calls into question the "liberty-security tradeoff" meme. Like them, he calls into question the few successes publicly identified with the NSA programs and worries, as they do, that the extraordinary rate of false positives means that the FBI is too often spending significant time and effort on leads that go nowhere.[145]

Bryce Newell, who is both an attorney and a doctoral student in information science, places the civil liberties question in a more theoretical frame.[146] Taking what he calls a "neo-republican" stance on the nature of liberty–namely, that liberty manifests itself in the ability of a people to self-govern, by reducing domination and the arbitrary exercise of power–Newell argues that surveillance is not necessarily inimical to liberty per se. Its legitimacy, however, requires that it be exercised for the public good and that the public have meaningful opportunities to challenge the secrecy in government that may prevent people from exercising genuine democratic oversight and control over their political representatives. He finds that idea honored more robustly in relevant decisions of the European Court of Human Rights than in U.S. courts, whose resistance to secrecy challenges he criticizes.

Given serious concerns from multiple angles that the Snowden leaks and accompanying document declassification have evoked, the issue is finally imposed: how might matters be improved? In the fall of 2013, President Obama convened a review group of academics and former intelligence officials to advise him on reform. Their efforts yielded 46 suggestions,[147] some of which the President has adopted.[148] These ideas, however, have hardly exhausted the need for further thinking.

---

[145] *Id.* at 469-471.

[146] Bryce Clayton Newell, *The Massive Metadata Machine: Liberty, Power, and Secret Mass Surveillance in the U.S. and Europe*, 10 ISJLP 481-522 (2014).

[147] PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES, LIBERTY AND SECURITY IN A CHANGING WORLD (Dec. 2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[148] *Transcript Of President Obama's Speech On NSA Reforms,* NPR.ORG (Jan. 17, 2014), http://www.npr.org/blogs/itsallpolitics/2014/01/17/263480199/transcript-of-president-obamas-speech-on-nsa-reforms; Fred Kaplan, *Pretty Good Privacy: The Three Ambitious NSA Reforms Endorsed by Obama, and the One He Rejected,* SLATE (Jan. 17, 2014), http://www.slate.com/articles/news_and_politics/war_stories/2014/01/obama_s_nsa_reforms_the_president_s_proposals_for_metadata_and_the_fisa.html.

Professor Nathan Sales, whose government service most recently includes a stint as Deputy Assistant Secretary for Policy Development in the Bush Department of Homeland Security, advocates the establishment of what he calls baseline rules for conducting "programmatic surveillance."[149] More than a number of other authors in this volume, he credits the value of such surveillance and thinks it unlikely to disappear. It is therefore perhaps unsurprising that he believes the NSA, as currently operating, already respects–though perhaps imperfectly–a number of the baseline principles he identifies. He does advocate that metadata surveillance be continued on the basis of clearer and more explicit statutory authority in order to maximize the potential for both effective congressional and judicial oversight. He would also like to see debates over the adoption of such programs become more transparent to the public and better informed. Perhaps his most innovative suggestion is the application to the NSA programs of the insight that internal bureaucratic controls might partially substitute for external judicial and congressional constraints as mechanisms for advancing privacy and civil liberties values.[150]

Professor Stephen Vladeck–although perhaps less sanguine about programmatic surveillance than Professor Sales–takes a cautionary stance on the potential for intensifying judicial review.[151] Post-9/11 litigation has been severely hamstrung by a combination of standing problems and the state secrets doctrine. Even if Congress enacted a workaround for the standing, it is not clear how routinely plaintiffs could challenge NSA programs absent a steady stream of further leaks. Proposals to make FISC hearings more adversarial hold more promise, but it remains unclear whether Article III would permit a designated advocate to appeal FISC orders to a higher court or whether it is possible to conduct an effectively adversarial system consistent with the level of secrecy that a system of foreign intelligence surveillance might well require.

Former FCC Chairman Reed Hundt takes a rather different tack.[152] No doubt reflecting his knowledge as a former telecommunications regulator, Mr. Hundt is careful to cast what most are calling NSA surveillance as a collaborative project between government and the private sector. He is emphatically concerned about the prospects for a

---

[149] Nathan Alexander Sales, *Domesticating Programmatic Surveillance: Some Thoughts on the NSA Controversy*, 10 ISJLP 523-550 (2014).

[150] *Id.* at 547-548.

[151] Stephen I. Vladeck, *Standing and Secret Surveillance*, 10 ISJLP 551-579 (2014).

[152] Reed E. Hundt, *Making No Secrets About It*, 10 ISJLP 581-598 (2014).

kind of "corporatism" he thinks inimical to "both economic and social freedom."[153] Mr. Hundt argues that it is, in fact, secrecy, rather than the fact of surveillance that is the fundamental problem with the current system. He proposes an ambitious list of reforms aimed at increasing what individuals know about their own targeting and what the public knows about the scope of government programs, past and present. Although his menu of suggestions includes an expansion of warrant requirements, the weight of his argument really goes to the public-ness of what the government is doing, reducing the likelihood of abuse once information has been collected, and better managing what could be the mind-boggling expense of managing security in the digital domain–what Mr. Hundt calls "the staggering expenditures of taxpayer funds."[154]

If Congress is to take on serious FISA modernization, however–with a level of interbranch deliberation and public debate as robust as in 1978–it could do no better than start with Professor Laura Donohue's article with the simple title, *FISA Reform*.[155] In an earlier work,[156] she has argued that a program entailing the interception of all international communications fails the reasonableness test of *Katz*; the compulsory involvement of private telecom companies and the failure to prevent overbreadth render the program unconstitutional. In this follow-up article, Professor Donohue maps out with extraordinary care the menu of issues now presented for the regulation of surveillance by the diversity of kinds of information at stake and the diversity of media through which information is accessed, transmitted and stored. She attends first to what might be called the front-end issues of how information is to be collected, by whom, and under what circumstances. She then considers back-end issues, that is, controls on how data are analyzed, used, retained, and transferred, as well as requirements for transparency, oversight and accountability. Although she does not purport in this paper to resolve these issues, her discussion is an invaluable roadmap to the policy terrain that any thoroughgoing FISA rewrite should have to traverse.

Hovering quite conspicuously over all these important questions is whether what might be called the "cybernation" of information–that is, the revolution in the digitizing of information with its profound

---

[153] *Id.* at 583.

[154] *Id.*.

[155] 10 ISJLP 599-639 (2014).

[156] Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*,37 HARV. J.L. & PUB. POL'Y 619-620 (2014).

impacts on information storage, processing, and dissemination–requires a comprehensive rethinking of the value, nature, and protection of privacy. It is thus fitting that our concluding essay, by the eminent sociologist Amitai Etzioni, elaborates what its author takes to four core principles of what he calls a liberal communitarian approach to cyber age privacy, along with a host of possible operational implications.[157] His paper functions as an invitation to view the NSA disclosures as an occasion for embracing a yet wider view, taking a systematic look at the principles we would wish to guide information policy in the cyber age.

VI. A CONCLUDING NOTE ABOUT EXECUTIVE POWER

The Snowden leaks and the subsequent Obama Administration declassifications have pointedly refocused Congress's attention on the prospects for FISA reform. Both our elected branches appear to be acting on the assumption that whatever legislation emerges will actually govern how the NSA operates[158]–whether its operations are affirmed in their current scope, legislatively restricted, or, least likely, authorized in yet more expansive terms. Professor Yoo, however, advances in his paper a theory of executive authority that also underlay his legal advice as a government official–a theory that casts significant doubt on the imperative of legislative observance by the executive branch. The core premise of his argument is as follows:

> The Constitution vests the President with the executive power and designates him Commander-in-Chief. The Framers understood these powers to place the duty on the executive to protect the nation from foreign attack and the right to control the conduct of military hostilities. To exercise that power effectively, the President must have the ability to engage in electronic surveillance that gathers intelligence on the enemy.[159]

---

[157] Amitai Etzioni, *A Cyber Age Privacy Doctrine: A Liberal Communitarian Approach*, 10 ISJLP 641-669 (2014).

[158] The Obama Administration is notably more reluctant than its predecessor to assert presidential power, even in national security setting, to act beyond what Congress enacts by way of statutory authority. Peter M. Shane, Executive Power, the Rule of Law and the Obama Administration (unpublished manuscript).

[159] Yoo, *supra* note 3, at 319 (footnotes omitted).

Professor Yoo argues that it follows from this position that the President does not need legislative authorization to conduct such surveillance as he deems necessary to protect the United States against foreign enemies; it follows further, in his view, that Congress may not place any binding limitations on that authority. The function of FISA, as Professor Yoo construes the Constitution, is neither to enable, nor to limit national security surveillance per se; it is only to prescribe a legal safe harbor within which the executive branch may both engage in national security surveillance and use its fruits as evidence in any criminal prosecutions that ensue.[160]

A great deal is packed into that argument, which is important to disentangle. First, putting aside controversial issues surrounding the supposition of presidential authority to determine with whom we are "at war" and of the consequent scope of commander-in-chief authority, it strikes me as quite plausible that the founding generation understood "executive power" to include some tacit authority to engage in intelligence work against foreign powers. After all, neither the durability of the new nation, nor even the congenial reception of other nations to the United States could be taken for granted in 1789. It is reasonable that the framers themselves would have read Article II as empowering the President to keep tabs on foreign powers and their agents as part of his inherent national security portfolio.

It does not follow from that observation, however, either that Congress could not regulate his surveillance of foreign powers, much less that the President would be deemed to have exclusive power beyond the regulatory authority of Congress to engage in the surveillance of Americans, especially in the absence of declared war. Even if some version of the latter power might be thought to exist absent a legislative charter, Congress's undoubted authority to regulate our networks of electronic communication give it the right, at its discretion, to legislate the circumstances under which Americans may be brought within the government's surveillance umbrella. There is no doubt that this is what Congress thought it was doing when it enacted the original FISA.[161]

---

[160] *Id.* at 301-326.

[161] "The conferees agree that the establishment by this act of exclusive means by which the President may conduct electronic surveillance does not foreclose a different decision by the Supreme Court. The intent of the conferees is to apply the standard set forth in Justice Jackson's concurring opinion in the Steel Seizure Case: 'When a president takes measures incompatible with the express or implied will of congress, his power is at the lowest ebb, for then he can rely only upon his own constitutional power minus any constitutional power of congress over the matter.' *Youngstown Sheet and Tube Co. v. Sawyer*, 343 U.S. 579, 637 (1952)." Foreign Intelligence Surveillance Act of 1978 Conference Report, H. REP. NO. 95-1720. at 35.

Prior to FISA, when Congress enacted its Title III procedure for criminal surveillance warrants after the *Katz* decision, Congress provided that "nothing contained in [Title III] or in section 605 of the Communications Act of 1934 shall limit the constitutional power of the President . . . to obtain foreign intelligence information deemed essential to the security of the United States."[162] But FISA replaced that statement with language dictating that FISA and the criminal code would be henceforth the "exclusive means" of conducting electronic surveillance. Congress amended the criminal code to read in unambiguous terms: "[P]rocedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted."[163] Congress had been confirmed in its authority to impose such a limitation by two Attorneys General, Edward Levi and Griffin Bell.[164]

Congress repeated its position in enacting the FISA Amendments Act of 2008. In the face of Justice Department opinions appearing to suggest either that FISA had not definitively limited the executive branch's surveillance authority or that the post-9/11 AUMF had implicitly augmented that authority, Congress reasserted the exclusivity point in Title 50 of the United States Code as well. FISA now reiterates the strict limitations on those statutory sources of authority on which the executive may rely to support electronic surveillance and adds that any additional authorities may be found only through subsequent "express statutory authorization," not through mere implication.[165]

It is imperative as a matter of democratic, constitutional self-governance that the executive branch acquiesce in Congress's view. Indeed, it may be this point–as much as the ex parte nature of FISC proceedings–that explains the seemingly odd disjuncture, noted above, between the FISC's apparent super-indulgence of counterintuitive statutory interpretations by the executive branch and its vigilance in the design and monitoring of provisions for minimization and other matters of implementation. That is, by

---

[162] Pub. L. No. 90-351, title III, § 802, 82 Stat. 213 (1968), repealed, Pub. L. 95–511, title II, § 201(a)–(c), 92 Stat. 1797 (1978).

[163] Pub. L. No. 95-11, title II, § 201(a)–(c), 92 Stat. 1797 (1978), codified at 18 U.S.C. § 2511(2)(f).

[164] H.R. REP. NO. 95-1283, pt. 1, at 24 (1978).

[165] Pub. L. No. 110-261, title I, § 102(a), 122 Stat. 2459, codified at 50 U.S.C. § 1812.

accepting executive branch statutory interpretations that bring its surveillance activities within the purview of statute, the court accomplishes two things it might well consider important from a "rule of law" point of view. First, it avoids sensitive questions of whether, notwithstanding FISA, the executive could pursue certain kinds of surveillance under inherent Article II authority–authority that the FISC would not be entitled to supervise. Second, the statutory rubric authorizes the FISC to impose limiting implementation requirements in the name of privacy which the court does monitor rigorously and in which the executive acquiesces–even, as with regard to bulk telephone records, where the court's authority to impose such requirements might be deemed questionable.

The FISC's institutional compromise, if I have correctly identified it, is hardly perfect. Its acquiescence in novel statutory interpretations looks like a disservice to a Congress that remains largely ignorant of those interpretations. The public forum surrounding legislative authorization is likely to be the only meaningful occasion for public deliberation on the proper contours for programs of electronic surveillance because there is quite likely to be no other context in which the executive branch will publicize the scope of what it thinks it needs to protect national security. If the FISC creates secret and unanticipated readings of Congress's handiwork, the value of such public deliberation is plainly called into question. And, of course, even if the NSA conscientiously follows the FISC's administrative requirements, the conscientious implementation of statutory authority that cannot be defended as a plausible statutory reading would still be an exercise in illegality.[166] But, as I have argued elsewhere, an executive branch that thinks its authority limited only by its unilateral assessments of its inherent discretionary powers is far more likely to overreach than an executive that thinks itself beholden to legislative authorization.[167] By helping to stabilize government surveillance practice within a statutory framework, the FISC may still be doing some significant service.

In the 1970s, it was the Church Committee that lent impetus to both the reorganization of intelligence oversight in Congress and the eventual enactment of FISA. Its investigation created a historical record that Americans could rely on as a basis for democratic debate about national security and intelligence gathering. Something similar

---

[166] Christopher Sprigman, *The NSA's Culture of 'Legal Compliance' Still Breaks the Law*, JUST SECURITY (Feb. 24, 2014), *available at* http://justsecurity.org/2014/02/24/nsas-culture-legal-compliance-breaks-law.

[167] PETER M. SHANE, MADISON'S NIGHTMARE: EXECUTIVE POWER AND THE THREAT TO AMERICAN DEMOCRACY 113-142 (2009).

should have happened in 2005-2006, when revelations about the Bush Administration made clear that government lawyers thought FISA did not constrain them. Instead, for better or worse–perhaps both–the official inquiry and public debate that should have preceded amendments to FISA instead were triggered only by massive unauthorized leaks that revealed NSA surveillance of staggering scope. The implications of the current debate are plainly profound for both our future security and long- cherished American values. It remains to be seen whether our national institutions are up to the challenge.